

## Best Available Copy

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276444

(43)Date of publication of application : 06.10.2000

(51)Int.Cl.

G06F 15/00  
H04L 9/32

(21)Application number : 11-076875

(71)Applicant : CANON INC

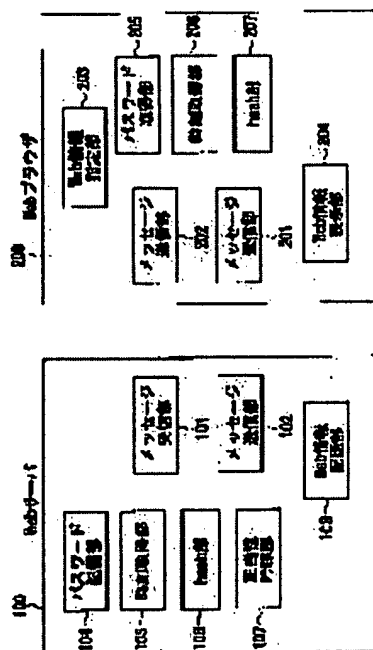
(22)Date of filing : 19.03.1999

(72)Inventor : KUROSAWA TAKAHIRO

**(54) COMMUNICATION EQUIPMENT, COMMUNICATION SYSTEM, AND COMPUTER READABLE STORAGE MEDIUM****(57)Abstract:**

**PROBLEM TO BE SOLVED:** To securely perform authentication by only performing unidirectional communication on a network once.

**SOLUTION:** In a Web browser 200, a first time from a time acquisition part 206 and a password from a password part 205 are operated in a hash part 207, and a message including this first operation result and the first time is transmitted from a message transmission part 202 to a Web server 100. In the Web server 100, the received first time and a password in a password storage part 104 are operated in a hash part 106 to obtain a second operation result. A validity examination part 107 compares a second time from a time acquisition part 105 with the first time, and it is decided that the receiver message is valid when the second time is later than the first time and the first operation result is matched with the second operation result.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-276444

(P2000-276444A)

(43) 公開日 平成12年10月6日 (2000.10.6)

| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I           | テームコード* (参考)      |
|---------------------------|-------|---------------|-------------------|
| G 0 6 F 15/00             | 3 3 0 | G 0 6 F 15/00 | 3 3 0 B 5 B 0 8 5 |
| H 0 4 L 9/32              |       | H 0 4 L 9/00  | 6 7 3 A 5 J 1 0 4 |
|                           |       |               | 6 7 3 D           |

審査請求 未請求 請求項の数14 O L (全 9 頁)

(21) 出願番号 特願平11-76875

(22) 出願日 平成11年3月19日 (1999.3.19)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 黒澤 貴弘

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 幸悦

Fターム(参考) 5B085 AC12 AE03 AE23

5J104 AA07 KA01 KA03 KA04 NA05

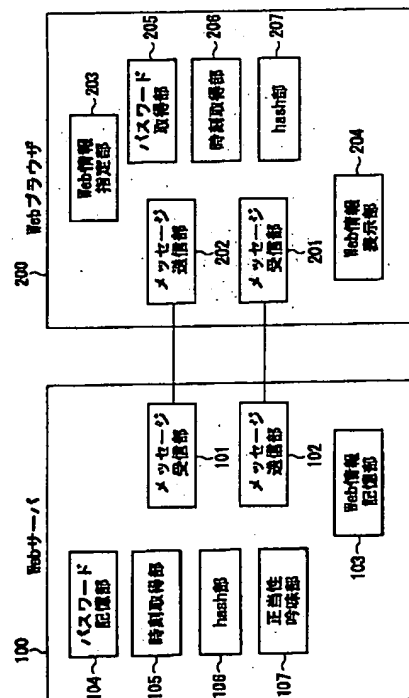
NA11 NA12 PA09

(54) 【発明の名称】 通信装置、通信システム及びコンピュータ読み取り可能な記憶媒体

(57) 【要約】

【課題】 ネットワーク上で単方向通信を1回行うだけで安全に認証を行うことができるようにする。

【解決手段】 Webブラウザ200において、時刻取得部206からの第1の時刻とパスワード部205からのパスワードとをhash部207で演算し、その第1の演算結果と上記第1の時刻を含むメッセージをメッセージ送信部202からWebサーバ100に送信する。Webサーバ100では、受信した第1の時刻とパスワード記憶部104のパスワードとをhash部106で演算して第2の演算結果を得る。そして、正当性吟味部107において、時刻取得部105からの第2の時刻と上記第1の時刻とを比較し、第2の時刻が第1の時刻より後で、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記受信したメッセージが正当であると判定する。



## 【特許請求の範囲】

【請求項1】 時刻を取得する時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算手段と、上記演算結果と上記時刻とを含むメッセージを作成して送信する送信手段とを設けたことを特徴とする通信装置。

【請求項2】 第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信手段と、上記受信時の第2の時刻を取得する時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを設けたことを特徴とする通信装置。

【請求項3】 上記判定手段は、上記第1の時刻と第2の時刻との差の時間が所定時間以内であり、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記メッセージが正当であると判定することを特徴とする請求項2記載の通信装置。

【請求項4】 上記第1の時刻を記憶する記憶手段を設け、上記判定手段は、次回に受信したメッセージに含まれる第1の時刻が上記記憶した第1の時刻より未来であるか否かを判定することを特徴とする請求項2記載の通信装置。

【請求項5】 上記メッセージは送信元情報を含み、複数の第1の通信装置にそれぞれ対応して上記所定時間を登録した登録手段を設け、上記判定手段は、上記送信元情報と対応する上記登録された所定時間と上記差の時間とを比較することを特徴とする請求項2記載の通信装置。

【請求項6】 時刻を取得する第1の時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した第1の時刻と入力されたパスワードとを不可逆に加工演算して第1の演算結果を出力する第1の演算手段と、上記第1の演算結果と上記第1の時刻とを含むメッセージを作成して送信する送信手段とを有する第1の通信装置と、上記メッセージを受信する受信手段と、上記受信時の第2の時刻を取得する第2の時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する第2の演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記第1の演算結果と第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを有する第2の通信装置とからなる通信システム。

【請求項7】 上記判定手段は、上記第1の時刻と第2の時刻との差の時間が所定時間以内であり、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記メッセージが正当であると判定することを特徴とする請求項6記載の通信システム。

【請求項8】 上記第2の通信装置に上記第1の時刻を記憶する記憶手段を設け、上記判定手段は、上記受信したメッセージに含まれる第1の時刻が上記記憶した第1の時刻より未来であるか否かを判定することを特徴とする請求項6記載の通信システム。

【請求項9】 複数の上記第1の通信装置が設けられ、各第1の通信装置は送信元情報を含む上記メッセージを送信し、上記第2の通信装置に上記複数の第1の通信装置にそれぞれ対応して上記所定時間を登録した登録手段を設け、上記判定手段は、上記送信元情報と対応する上記登録された所定時間と上記差の時間とを比較することを特徴とする請求項6記載の通信システム。

【請求項10】 時刻を取得する時刻取得処理と、パスワードを入力するパスワード入力処理と、上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算処理と、

上記演算結果と上記時刻とを含むメッセージを作成して送信する送信処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項11】 第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信処理と、

上記受信時の第2の時刻を取得する時刻取得処理と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算処理と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項12】 上記判定処理は、上記第1の時刻と第2の時刻との差の時間が所定時間以内であり、かつ上記第1の演算結果と第2の演算結果とが一致したとき上記メッセージが正当であると判定することを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項13】 受信したメッセージに含まれる時刻を記憶する記憶処理を上記プログラムに設け、上記判定処理は、受信したメッセージに含まれる時刻が上記記憶した時刻より未来であるか否かを判定することを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項14】 上記メッセージは送信元情報を含み、上記判定処理は、複数の送信元にそれぞれ対応して予め登録された上記所定時間のうちの上記送信元情報と対応する所定時間と上記差の時間とを比較することを特徴と

する請求項1記載のコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク上のサーバが遠隔地にあるクライアントの正当性を認証するようにした通信システムに用いて好適な、上記サーバ及びクライアントが用いる通信装置、この通信装置を有する通信システム及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

【従来の技術】近年、以下に列挙するような認証に関する技術あるいは製品が提供されるようになってきた。

・ 一方関数を用いた認証方法

入力を不可逆に加工する関数を用いる。これは、その関数の出力結果から関数の入力(引数)となった情報を推測することが難しい関数である。例えばRFC1321に示されるMD5などの関数であり、Message Digestの作成などにも利用される。実装上はハッシュ(hash)関数として知られる関数が利用されることもある。

【0003】・ one-time パスワード型認証方法  
インターネットなどのネットワークの発達にともなう、ネットワーク上を流れるパケットを覗き見るなどの手法によるアカウントやパスワードの不正取得あるいは不正利用が行なわれるようになってきた。AT&TによるOTPなどに代表されるone-time パスワード型認証方法は、このような不正行為に対して防衛する目的で用いられている。この方法では、ネットワーク上を流れるパスワード情報は毎回変わるよう設計されている。

【0004】・ challenge response 型認証方法

上記と同様の目的で、challenge response 型認証方法が用いられている。これは、接続リクエストを発行したクライアントに対してサーバ側から提供されるchallenge データを、クライアント側でパスワードのhashに組み入れることで、パスワード自体は変化しないにも関わらず、hash結果のresponse データの値が何回変わるように設計されている。このため、パスワード情報の送付に利用したパケットがネットワークの途中で覗き見されることがあっても、同一のパスワード情報が有効になることは、確率的に非常に少なく、パスワードの安全性が高められる〔図1(b)参照〕。

【0005】・ NTP(Network Time Protocol)

ネットワーク接続されたコンピュータの内部時計を正しく調整するためのプロトコルとして、TP(Network Time Protocol; RFC1119)

が使われている。

【0006】

【発明が解決しようとする課題】しかしながら、従来のchallenge response 型認証方法では、クライアントからの接続要求を受けてから。サーバ側で生成したchallenge データをクライアント側に送り返し、さらにクライアント側でそのchallenge データからresponse データを生成してサーバ側に送るという手続きを取るために、一回の接続要求の認証のために、最低3回の通信パケットの送受信を必要としている。このことは、インターネットなどのように通信コストの大きなネットワークで利用されるアプリケーションの場合には、その応答性を落とすという問題があった。

【0007】本発明は、上記の問題を解決するために成されたもので、一回の接続要求の認証のために、一回の通信パケットの送受信で済ませることができるようになることを目的としている。

【0008】

【課題を解決するための手段】上記の目的を達成するために、本発明による通信装置においては、時刻を取得する時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算手段と、上記演算結果と上記時刻とを含むメッセージを作成して送信する送信手段とを設けている。

【0009】また、本発明による他の通信装置においては、第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信手段と、上記受信時の第2の時刻を取得する時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを設けている。

【0010】また、本発明による通信システムにおいては、時刻を取得する第1の時刻取得手段と、パスワードを入力するパスワード入力手段と、上記取得した第1の時刻と入力されたパスワードとを不可逆に加工演算して第1の演算結果を出力する第1の演算手段と、上記第1の演算結果と上記第1の時刻とを含むメッセージを作成して送信する送信手段とを有する第1の通信装置と、上記メッセージを受信する受信手段と、上記受信時の第2の時刻を取得する第2の時刻取得手段と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する第2の演算手段と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記第1の演算結果と第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定手段とを有する第

5

2の通信装置とを設けている。

【0011】また、本発明による記憶媒体においては、時刻を取得する時刻取得処理と、パスワードを入力するパスワード入力処理と、上記取得した時刻と入力されたパスワードとを不可逆に加工演算する演算処理と、上記演算結果と上記時刻とを含むメッセージを作成して送信する送信処理とを実行するためのプログラムを記憶している。

【0012】また、本発明による他の記憶媒体においては、第1の時刻とパスワードとを不可逆に加工演算した第1の演算結果と上記第1の時刻とを含むメッセージを受信する受信処理と、上記受信時の第2の時刻を取得する時刻取得処理と、上記第1の時刻と所定のパスワードとを不可逆に加工演算し第2の演算結果を出力する演算処理と、上記第1の時刻と第2の時刻とを比較し、その比較結果に応じて上記受信した第1の演算結果と上記第2の演算結果とを比較することにより上記メッセージの正当性を判定する判定処理とを実行するためのプログラムを記憶している。

【0013】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。

(第1の実施の形態) 図2は、本発明をWorld Wide Web(以下、Webと略す)サーバ及びクライアントとしてのWebブラウザに用いた場合の通信システムを示すブロック図である。図2において、100は本実施の形態による認証機能を有するWebサーバ、200は本実施の形態によるメッセージを送信するWebブラウザである。

【0014】Webサーバ100とWebブラウザ200はそれぞれネットワーク300に接続され、Webブラウザ200からネットワーク300を介してWebページ情報のリクエストがWebサーバ100へメッセージとして送られる。Webサーバ100では、まず、受信したメッセージの正当性を判断し、正当であることが認められると、Webブラウザ200へ上記リクエストされたWebページ情報を送付する。Webブラウザ200では、受信したWebページ情報を表示することができる。

【0015】尚、この図2のネットワーク300は、企業あるいは組織内で運用されるイントラネットである場合もあり、あるいは広く世界をつないでいるインターネットである場合もある。

【0016】図3はWebサーバ100を動作させるハードウェアの構成例を示すものであり、一般のコンピュータシステムで構成されている。即ち、プログラムを格納したHD装置10及びメモリ11、ネットワーク300と接続するためのネットワークI/F12、プログラムによる各種の処理を実行するCPU13、プログラムを媒体からロードするためのFD装置14、周辺コン

6

ローラ15、表示ボード16、マウス17、キーボード18、ディスプレイ装置19などから構成されている。

【0017】図4はWebブラウザ200を動作させるハードウェアの構成例を示すものであり、一般のコンピュータシステムで構成されている。即ち、プログラムを格納したHD装置20及びメモリ21、ネットワーク300と接続するためのネットワークI/F22、プログラムによる各種の処理を実行するCPU23、プログラムを媒体からロードするためのFD装置24、周辺コン

ローラ25、表示ボード26、マウス27、キーボード28、ディスプレイ装置29などから構成されている。

【0018】図5はWebサーバ100とWebブラウザ200の構成を模式化したブロック図である。これらの各部の処理を実装したプログラムは、図3、図4のハードウェア構成上では、HD装置10、20やメモリ11、21あるいはFD装置14、24に格納され、必要に応じてCPU13、23で実行される。

【0019】Webサーバ100は、ネットワーク300上からデータを受け取るメッセージ受信部101と、ネットワーク上にデータを送り出すメッセージ送信部102と、個々のWebページ情報を記憶しておき、求めに応じてそれらを取り出すためのWeb情報記憶部103とからなる通常のWebサーバの構成に加えて、予めパスワードが登録されたパスワード記憶部104と、コンピュータ内の時刻情報を取得するための時刻取得部105と、不可逆な加工演算を行う一方関数を提供するhash部106と、入力された時刻情報やhash結果から要求の正当性を判断するための正当性吟味部107とから構成される。

【0020】また、Webブラウザ200は、ネットワーク上からデータを受け取るメッセージ受信部201と、ネットワーク上にデータを送り出すメッセージ送信部202と、ユーザの求めるWeb情報を指定するURLなどを得るためのWeb情報指定部203と、受信したWebページ情報を表示するためのWeb情報表示部204とからなる通常のWebブラウザの構成に加えて、キーボードなどの入力装置からユーザ固有のパスワードを得るためのパスワード取得部205と、上記Webサーバ100と同様の時刻取得部206と、上記Webサーバ100と同一のhash部207とから構成される。

【0021】図6はWebブラウザ200が実装したプログラムの処理を示すフローチャートである。Webブラウザ200は、Webサーバ100にアクセスしようとする際、まずS1001ステップ(以下、ステップ略)で、Web情報取得部203からURLなどのWeb指定値を得る。次にS1002で、パスワード取得部205からパスワードを得る。続いてS1003で、時刻取得部206から時刻を得る。そしてS1004

10

20

30

40

50

で、それらのパスワードと時刻をhash部207によってhashする。

【0022】さらにS1005で、そのhash結果に上記時刻、ユーザ名、Web指定情報を添えてメッセージ送信部202からアクセス要求をWebサーバ100に送る。その後、S1006でWebサーバ100からの返答を待つ。そして、Webサーバ100でメッセージの正当性が認められるとWebサーバ100からページ情報が送信されるので、S1007で、メッセージ受信部201によりWebサーバ100からのWebのページ情報を受け取る。続いてS1008で、Webのページ情報をWeb情報表示部204で表示する。

【0023】図7は、Webサーバ100が実装したプログラムの処理を示すフローチャートである。最初にS2001で、Webブラウザ100からのアクセス要求を待つ。S2002で、メッセージ受信部101からメッセージを得る。次にS2003で、メッセージのユーザに相当するパスワードを、パスワード記憶部104から取り出す。続いてS2004で、時刻取得部105からWebサーバ側の受信時刻T1を得る。

【0024】そしてS2005で、受信したメッセージからWebブラウザ側の時刻T2を取り出す。またS2006で、パスワード記憶部104から得られたパスワードと上記時刻T2とを、S1004と同様の手順でhash部106により計算し、そのhash結果H1を得る。また、メッセージからhash結果H2を取り出す。

【0025】そしてS2007で、上記時刻T1、T2及びhash結果H1、H2を正当性吟味部107で検討し、認証の可否を決定する。そしてS2008で、認証が正当であるならば、メッセージ内のWeb指定情報から求められるWebページ情報をメッセージ送信部102によりWebブラウザ200に送信する。また、認証が正当でないならばその旨返答する。最後にS2001に戻り、次のアクセス要求を待ち合わせる。

【0026】図8は、一方向関数を提供するhash部106及びhash部207の処理を実装したプログラムの処理を示すフローチャートである。ここでは、説明を簡単にするために、入力となるパスワードと時刻情報を文字列で表現し、かつ一方向関数として、RFC1321に示されるMD5関数を利用する場合について述べる。まずS3001で、受け取ったパスワードと時刻情報を文字列化する。時刻情報に関しては、例えば、「1998/Jan/05.13:34:20」のような形式で表現するものとする。

【0027】次にS3002で、文字列化したパスワードと時刻情報を結合してMD5関数へ入力する。そしてS3003で、MD5関数の出力をhash結果とする。例えば、パスワード「paspaspas」、時刻「1998/Jan/05.13:34:20」と表さ

れる文字列を結合してMD5に入力した場合、次のような出力が得られる。MD5(“paspaspas1998/Jan/05.13:34:20”) = “0e47e121d048065433bbf8eed3446258” 従って、上記「0e47e121d048065433bbf8eed3446258」がhash結果となる。

【0028】図9は、正当性吟味部107の処理を実装したプログラムの処理を示すフローチャートである。正当性吟味部107は、送られてきたメッセージに含まれる時刻T2とWebサーバ内の時刻T1、及び送られてきたメッセージに含まれるhash結果H2とWebサーバ内に記憶していたパスワードから生成したhash結果H1とを入力として与えられ、メッセージの正当性を判定するブール値を回答する。

【0029】まずS4001で、送られてきたメッセージ内の時刻T2とWebサーバ側の時刻T1とを比較し、T2がT1よりも過去であるならば、次のステップに進み、過去でないならば、FALSEを回答する。次にS4002で、送られてきたメッセージ内のhash結果H2とWebサーバ内に記憶していたパスワードから生成したhash結果H1とを比較し、一致したならば次のステップに進み、一致しないならば、FALSEを回答する。次にS4003で、TRUEを回答する。

【0030】本実施の形態では、パスワードと時刻とを入力としてhashしているが、これに加えて、ユーザ名をhash部の入力に追加してもよい。また本実施の形態では、Webブラウザを独自プログラムとして説明したが、Netscape社のNavigatorやMicrosoft社のInternet Explorerなどのような汎用のWebブラウザ上で動作するJAVAプログラムやActiveXプログラムで実装することもできる。

【0031】以上述べたように、ネットワーク上で利用されるプログラムの認証を行う場合に、パスワードのhash部に、時刻情報をも追加入力することにより、challenge-response型認証よりも少ない通信コストでありながら同程度の安全性を提供することができる。

【0032】(第2の実施の形態) 第1の実施の形態では、正当性吟味部107は、前記S4001において、送られてきたメッセージに含まれる時刻T2がWebサーバ内の時刻T1よりも過去である場合に正当と判定していたが、本実施の形態では、この部分に加えて、「同一ユーザの前回のアクセス要求のメッセージに含まれていた時刻T3よりも、今回のメッセージに含まれる時刻T2がより未来である場合のみ正当」と判定する点に特徴がある。

【0033】このためには、前記S4001の処理とS4002の処理との間に、以下のようなステップS42

10

20

30

40

50

01を挿入することで実現できる。S4201では、送られてきたメッセージ内の時刻T2と、Webサーバ内に記憶されているユーザ情報内の前回アクセスの時刻T3とを比較し、今回のメッセージに含まれる時刻T2の方が未来であるならば、その時刻T2をユーザ情報内の前回のアクセス時刻として登録し、次のステップに進む。反対に、今回のメッセージに含まれる時刻の方が過去であるならば、FALSEを回答する。これにより、Webブラウザからのメッセージの正当性をより厳密にチェックすることができる。

【0034】(第3の実施の形態)第1の実施の形態では、正当性吟味部107は、S4001において、送られてきたメッセージに含まれる時刻T2がWebサーバ内の時刻T1よりも過去である場合に正当と判定していたが、本実施の形態では、この部分を「T1とT2の時刻との差の絶対値が予め規定された時間内にある場合のみ正当」と判定する点に特徴がある。

【0035】このためには、S4001の処理を以下のようなステップS4101に変更することで実現できる。尚、ここでは、「予め規定された時間」を20分間として説明するが、これ以外の時間であってもよい。また、固定的に規定される値ではなくWebサーバの起動時に初期設定される値であってもよい。S4101では、送られてきたメッセージ内の時刻とWebサーバの時刻との差分を計算し、その絶対値の大きさが20分間以内ならば、次のステップに進む。20分間を超えるならばFALSEを回答する。

【0036】これにより、コンピュータ間に時間のズレがあった場合にも対応可能となり、かつ充分過去に生成されたメッセージは、不正であるとの判定が可能となる。しかも、時刻情報をアクセス制限にも利用できることから、一層柔軟なアクセス制限が可能となる。

【0037】尚、ここでは、「予め規定された時間」を固定的に説明しているが、以下に示すようなユーザ名と規定時間との対応表を作成することで、ユーザ毎に可変の規定時間を適用することができる。また、下記の表における規定時間が0であった場合には、無条件にTRUEを回答するようにしてもよい。

【0038】

| 規定時間(分) | ユーザ名     |
|---------|----------|
| 50      | Akiyama  |
| 0       | Katura   |
| 20      | Kurosawa |
| 10      | Sakamoto |
| 120     | Tamura   |
| 50      | Yamamoto |

【0039】次に本発明の他の実施の形態としての記憶媒体について説明する。本発明をCPUとメモリやHD装置等でコンピュータシステムに構成する場合、上記メモリやHD装置等は本発明による記憶媒体を構成する。

即ち、前述した各実施の形態で説明したフローチャートによる動作を実行するためのソフトウェアのプログラムコードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のCPUが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【0040】また、この記憶媒体としては、ROM、RAM等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをCD-ROM、フロッピーディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

【0041】従って、この記憶媒体を各実施の形態で説明したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0042】また、コンピュータ上で稼働しているOS等が処理の一部又は全部を行う場合、あるいは記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるCPU等が処理の一部又は全部を行う場合にも、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0043】

【発明の効果】以上説明したように、本発明によれば、クライアント側の通信装置において、ネットワーク上での認証要求を目的とするパスワードのhash(不可逆な加工)時に時刻情報も一緒にhashし、hash結果と時刻とを含むメッセージを作成して、サーバ側の通信装置に送信するようにしたので、クライアント側のコンピュータ内の単調に増加する時刻情報を利用することにより、単方向に1回通信を行うだけで容易に認証を行うことができる。また、同じ認証情報が重複して使用されることがないので、従来のchallenge-response型認証よりも通信コストを少なくしながら、かつ同程度の安全性を得ることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態による認証方法と従来のchallenge-response型認証方法を説明するための構成図である。

【図2】本発明が適用されるネットワークシステムを示すブロック図である。

【図3】Webサーバのハードウェア構成例を示すブロック図である。

【図4】Webブラウザのハードウェア構成例を示すブ

11

12

ロック図である。

【図5】WebサーバとWebブラウザの構成を模式的に示すブロック図である。

【図6】Webブラウザの処理を示すフローチャートである。

【図7】Webサーバの処理を示すフローチャートである。

【図8】hash部の処理を示すフローチャートである。

【図9】正当性吟味部の処理を示すフローチャートである。

【符号の説明】

10、20 HD装置

11、21 メモリ

13、23 CPU

14、24 FD装置

18、28 キーボード

100 Webサーバ

101 メッセージ受信部

102 メッセージ送信部

103 Web情報記憶部

104 パスワード記憶部

105 時刻取得部

106 hash部

107 正当性吟味部

200 Webブラウザ

201 メッセージ受信部

202 メッセージ送信部

203 Web情報指定部

204 Web情報表示部

205 パスワード取得部

206 時刻取得部

207 hash部

300 ネットワーク

T1 Webサーバ内の時刻

T2 送られてきたメッセージに含まれる時刻

T3 前回の正当なメッセージに含まれる時刻

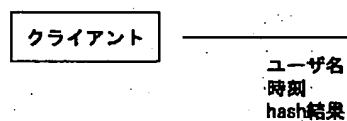
H1 Webサーバ中に記憶していたパスワードから生成したhash結果

20 H2 送られてきたメッセージに含まれるhash結果

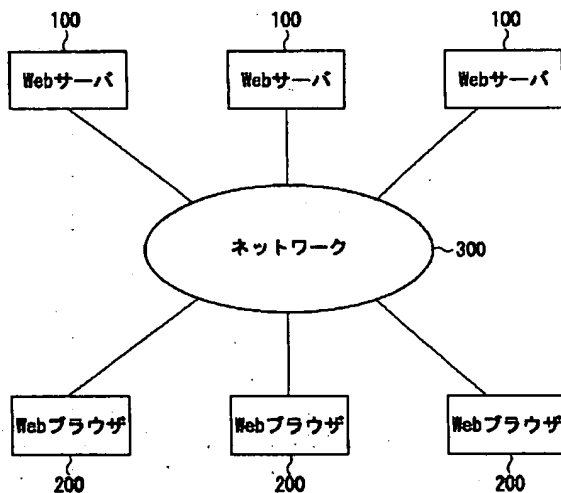
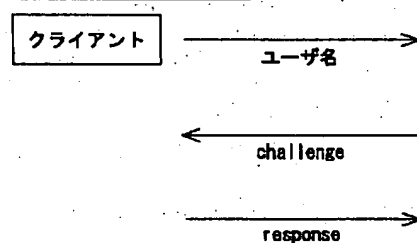
【図1】

【図2】

(a) 【本方式】

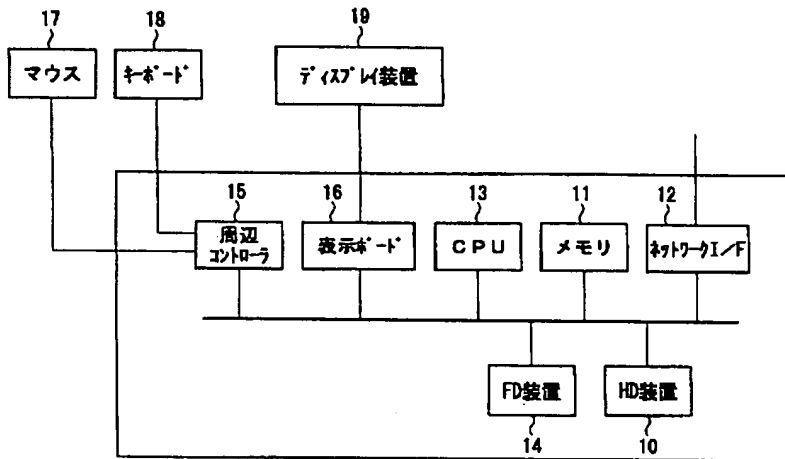


(b) 【challenge-response方式】

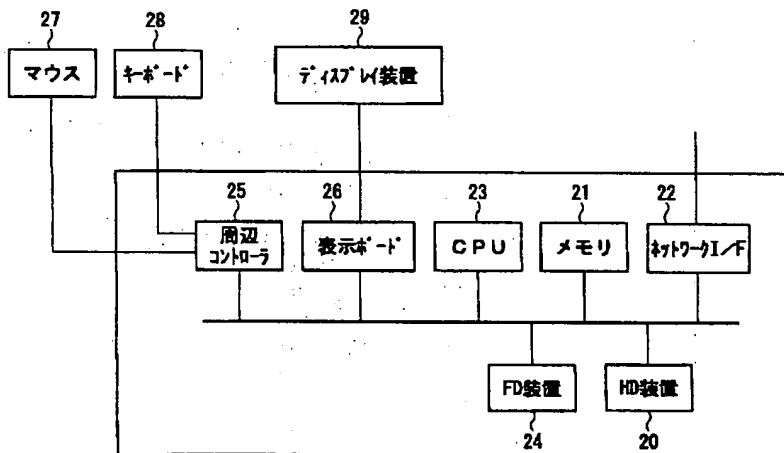




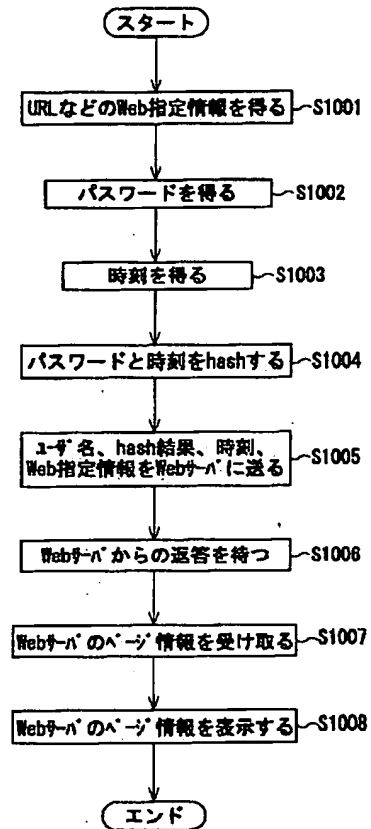
【 図3 】



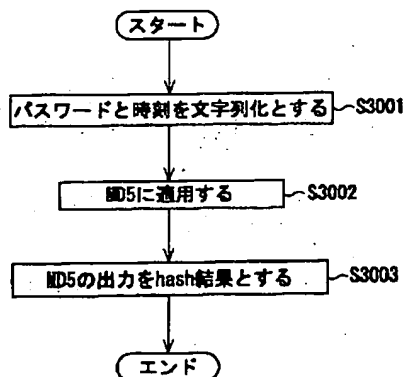
【 図4 】



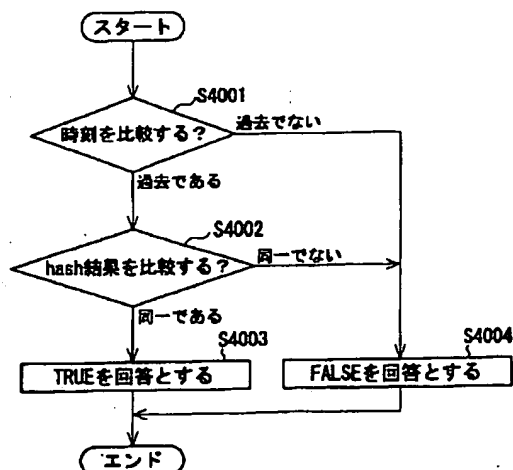
【 図6 】



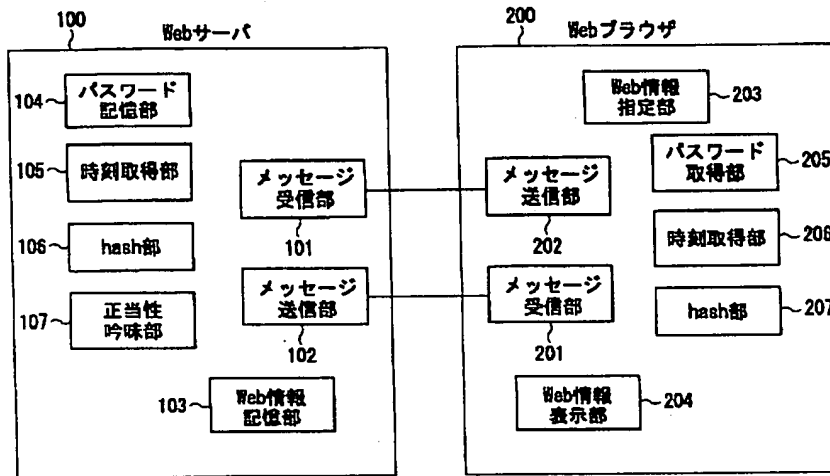
【 図8 】



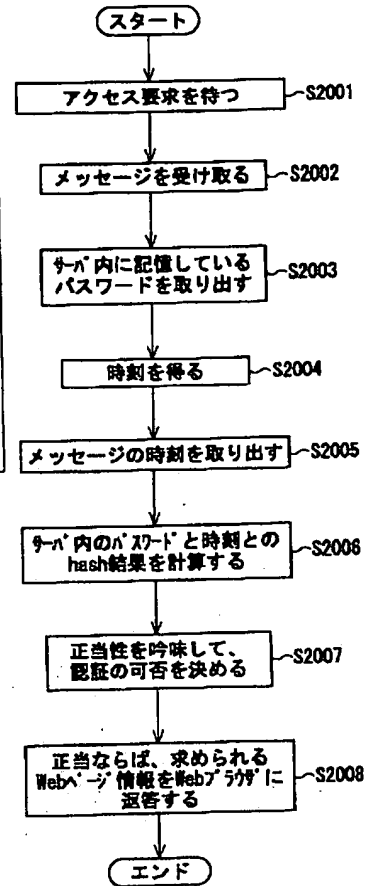
【 図9 】



【 図5 】



【 図7 】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**